Bruce C. Fox (*pro hac vice forthcoming*)
bruce.fox@obermayer.com
Hugh T. McKeegan (*pro hac vice forthcoming*)
hugh.mckeegan@obermayer.com
OBERMAYER REBMANN MAXWELL & HIPPEL LLP
525 William Penn Place, Suite 1710
Pittsburgh, PA 15219
Tel: (412) 566-1500
Fax: (412) 281-1530

Chaka Okadigbo (CA State Bar No. 224547)
cokadigbo@hkm.com
HKM EMPLOYMENT ATTORNEYS LLP
700 S. Flower Street, 10th Floor
Los Angeles, California 90017
Telephone/Facsimile: (213) 431-6209

Attorneys for Plaintiff Michael Stern

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA—SAN JOSE DIVISION

MICHAEL E. STERN, *Plaintiff* v. VECTRA AI, INC., *Defendant*	Case No.: _____ **COMPLAINT FOR DAMAGES** DEMAND FOR JURY TRIAL

Plaintiff Michael E. Stern states as follows:

NATURE OF THE ACTION

1. This action arises from Defendant Vectra AI, Inc.'s ("Vectra") unlawful treatment of Plaintiff Michael E. Stern, who worked for Vectra as a Regional Director, focusing on cybersecurity software sales to Department of Defense customers.

2. The relationship between Stern and Vectra was marred by Vectra's false representations and unethical and unlawful business practices from the outset. When Vectra recruited Stern in 2021, it falsely represented the viability of its software sales pipeline of Department of Defense customers and recklessly misrepresented that it was close to obtaining FedRAMP certification—a prerequisite to selling any cloud-based software to the federal government. In reality, Vectra had yet to even begin the FedRAMP certification process. Vectra also falsely represented the amount of commission payments (approximately $500,000) that Stern could expect to receive for these misrepresented sales opportunities in the pipeline.

3. Next, following third-party testing of Vectra's cybersecurity software, which disclosed glaring weaknesses in Vectra's ability to detect even basic cyber-attacks, Stern raised the alarm about the software's vulnerability and urged Vectra management to disclose the results of the tests to its federal government customers as well as prospective customers in the Federal sales pipeline. In response, Vectra

acted with resistance and hostility. Vectra failed to report the test results, although its software had already been deployed to protect military and intelligence computer networks vital to national security from cyber-attacks. Vectra instead fired Stern in direct retaliation for his persistent efforts to seek corrective action.

4. Finally, even after terminating his employment, Vectra continued its campaign against Stern, and intentionally disrupted his prospective employment opportunity with Vectra's competitor, DarkTrace.

THE PARTIES

5. Plaintiff Michael Stern is an adult individual residing at 811 North Orkney Street, Philadelphia, PA 19123. Stern is a decorated military veteran who served as a Naval Aviator for more than nine years, seeing active combat duty during Operation Desert Storm. He has more than 20 years of experience in software and IT sales, including sales to customers in the federal government, particularly within the Department of Defense. At all relevant times, Stern held an active Top Secret clearance, which required him to report any potential breaches of national security

6. Defendant Vectra AI, Inc. is a Delaware corporation with its principal place of business located at 550 S. Winchester Blvd., Suite 200, San Jose, California, 95128. Vectra develops and markets cybersecurity software and services to civilian and military customers in both the federal government and private industry in the United States and to governments and private industry around the world.

JURISDICTION AND VENUE

7. Under 28 U.S.C. § 1331, this Court has subject matter jurisdiction over Stern's claim under the anti-retaliation provision of the False Claims Act, 31 U.S.C. § 3730(h) (First Cause of Action), because it is a claim arising under the laws of the United States.

8. Under 28 U.S.C. § 1332, this Court has subject matter jurisdiction over Stern's California state law claims (Second, Third, Fourth, and Fifth Causes of Action) because there is complete diversity between the parties and the amount in controversy exceeds $75,000.

9. This Court has personal jurisdiction over Defendant Vectra because it maintains its principal place of business in this district.

10. Venue is proper in this district under 28 U.S.C. § 1391 because Defendant's principal place of business is in this district.

FACTUAL BACKGROUND

A. Vectra touts its product as providing cutting-edge cybersecurity.

11. Vectra Cognito (now known as "Vectra Threat Detection and Response Platform") (hereinafter the "Vectra Platform"), is a software product that purports to detect cybersecurity threats in users' computer networks.

12. The Vectra Platform is in place in various democratic governments and companies around the world and its role in preserving geopolitical stability is not inconsequential.

13. The Vectra Platform monitors activity on a user's network and, utilizing a set of proprietary algorithms and machine learning processes, identifies abnormal behavior linked to potential adversarial actions. Once such activity is detected, the Vectra Platform "alerts" the user to a potential security threat.

14. In other words, the Vectra Platform "learns" the typical flow of information to, from, and within a user's network and, by applying various supervised and unsupervised AI detection models, supposedly can alert the user to deviations from baseline or other abnormalities which may be indicative of a cyber-attack or other adversarial action against its network.

15. Vectra advertises the Vectra Platform as being superior to its competitors' products for two primary reasons. First, by focusing on "behaviors," Vectra claims that the Vectra Platform can detect previously unknown threats that legacy "signature"-based detection software cannot. Second, Vectra claims that its platform is less "noisy"—*i.e.*, the Vectra Platform returns many fewer "false positives" than its competitors.

16. In short, Vectra claims that its product allows users to "see" threats other products do not and aids in response speed by eliminating the need to sift through mountains of data.

17. Vectra has successfully marketed the Vectra Platform to customers in both government and private industry, in the United States and around the world. Before Stern's termination, the Vectra Platform was in use by various prominent U.S. military and security agencies and other governmental entities.

18. Upon information and belief, Vectra's relationships with federal government customers were worth up to several million dollars of annual recurring revenue to the company.

19. Furthermore, at the time of Stern's firing, Vectra was pursuing several further large-scale opportunities across the federal government, including those within the defense and intelligence spheres.

20. For example, the Vectra Platform was part of every major bidder's proposal for a U.S. military solicitation for next-generation cyberdefense. If awarded to one of Vectra's partners, the proposal would result in the Vectra Platform being widely deployed across the world in U.S. military applications.

B. Vectra recruited Stern to join its federal government sales team on false pretenses.

21. Stern was recruited to Vectra by Brian Davis, Vectra's then-Director of Federal Sales, and Marty Sanders, Vectra's Senior Vice President Americas, for a position in Vectra's sales team as Regional Director – Federal DoD.

22. At the time, Stern was employed by Rubrik, Inc., a company that provides data management and recovery software, as its Defense Department Sales Leader.

23. In his four-year career with Rubrik, Stern had successfully built the company's business with the Department of Defense to approximately 30 million of yearly recurring revenue.

24. In his role at Rubrik, Stern was paid on a 50/50 compensation plan, meaning half of his regular compensation came in form of base salary, with the other half coming from sales commissions.

25. Stern's base salary at Rubrik was approximately $190,000.

26. Stern was also eligible to receive commissions and bonuses for exceeding his yearly sales quota, stock options, and other benefits.

27. As part of their recruiting pitch to Stern, Davis and Sanders both made material representations to Stern about the amount and viability of Vectra's sales pipeline with customers in the defense sphere and the status of Vectra's efforts to obtain key certifications.

28. Stern would only later learn that those representations were wholly false.

29. During a two-hour meeting in or around August 2021, Davis provided Stern with detailed information about the Defense Department sales pipeline, including a number of large-scale deals that he claimed Stern would inherit should he accept employment with Vectra.

30. Davis listed many of these deals as being "committed," which typically means that a software vendor has obtained at least a verbal commitment that a deal will close.

31. The "committed" deals that Davis described to Stern included large scale deals with the U.S. Army and the U.S. Navy, and a prominent civilian defense agency command.

32. Indeed, Davis represented to Stern that one of the Navy deals was "committed."

33. Not only was the Navy deal not "committed" in any sense of the word at the time Davis described the opportunity to Stern, on information and belief, the Navy has to date yet to award any contract for the solicitation.

34. Davis further represented that a prospective application run by the Pentagon was in the pipeline for over $2.5 million.

35. Davis assured Stern that these deals would close before the end of the 2021 fiscal year and would therefore entitle Stern to substantial commissions.

36. Sanders also independently assured Stern of the viability of these deals, and represented that Stern stood to earn approximately $500,000 in commissions once they closed.

37. In addition, Davis and Sanders both represented to Stern that Vectra would soon obtain FedRAMP certification, which is a necessary requirement for selling cloud-based software to federal government customers.

38. Sanders also promised to provide Stern with adequate funding for three consultants and an inside salesperson to assist him with business development for Vectra.

39. Enticed by these representations, and by Vectra's impressive list of federal clients, Stern accepted an offer of employment with Vectra on September 13, 2021.

40. Like Rubrik, Vectra paid Stern on a 50/50 compensation plan.

41. Stern's base salary at Vectra was $185,000.

42. Stern was also eligible to receive commissions and bonuses for exceeding his yearly sales quota and was awarded stock options to purchase 27,500 shares of Vectra stock that would fully vest over four years.

43. As a consequence of accepting Vectra's employment offer, in addition to salary, bonuses, commissions, and continued employment by Rubrik, Stern forfeited significant unvested shares of Rubrik stock, in the form of restricted stock units ("RSUs") worth in excess of $900,000 based on pre-IPO market conditions at the time.

44. Stern was further forced to exercise his earned options, which cost him approximately $29,700, as well as generating a taxable event with the State of Pennsylvania and City of Philadelphia in excess of $18,000.

45. Stern began working for Vectra on October 18, 2021.

46. He soon learned that the reality at Vectra did not align with the pre-employment representations made to him by Davis and Sanders.

47. Within a few weeks of starting at Vectra, Stern discovered that Vectra was not, in fact, "close" to obtaining FedRAMP certification.

48. In reality, Vectra had yet to even begin the lengthy and rigorous FedRAMP certification process.

49. Stern also learned that the "pending deals" he was supposed to inherit upon joining Vectra would not close before the end of the 2021 fiscal year—indeed, many of those deals were never qualified properly and would never close at all.

50. In particular, Stern learned that as much as 90% of the alleged deals in his territory sales pipeline failed to meet minimum standards of sales qualifications, despite being identified as "committed" deals by Davis.

51. Because these alleged deals did not meet minimum qualifications, Stern was obligated to shut them down.

52. An example of this was an Army deal that was expected to close in late 2021 for almost $1.5 million. This particular deal was listed as being in a "committed" stage. Not only did the deal not close in late 2021 (per Sanders and Davis), it never closed at all due to failure to properly qualify the actual available budget, the agreement to purchase from customer, and any relevant information regarding necessary steps to close the deal.

53. Stern met with the economic buyer for Army in late 2021, Lt. Colonel Michael Lind, who confirmed that the budget was never promised in the amount that was communicated to Stern, nor was there any real budget at all. This was later reiterated by Lind's successor, Lt. Colonel Brad Son.

54. Losing these purported "deals" eliminated in excess of $6,000,000 in revenue from Stern's territory sales pipeline, causing Stern to lose more than $500,000 in prospective commissions.

55. Notably, Davis was fired within months of Stern starting at Vectra, due in part to his practice of listing deals as "committed" when, in fact, such deals were not.

56. Moreover, despite Sanders' assurances that Vectra would provide Stern with funding for three consultants to support business development and an inside salesperson, Vectra—only after months of pressure from Stern—contracted with two consultants.

57. Hence, within a few months of starting at Vectra, Stern was effectively in the unexpected position of needing to rebuild Vectra's sales pipeline of Department of Defense prospects from scratch, and without the support Sanders had promised him.

58. Nevertheless, Stern worked diligently to develop Vectra's business with federal government customers.

59. Indeed, by June 2022, Stern had secured the critical agreement of the Small Business Administration to serve as Vectra's sponsoring agency for the FedRAMP certification process.

C. Testing by the National Cyber Range demonstrates critical weaknesses in the Vectra Platform.

60. Stern's situation worsened in February 2022, however, when he learned the results of testing performed on the Vectra Platform by the National Cyber Range ("NCR").

61. NCR is a third-party testing and evaluation entity contracted by the United States government to, among other tasks and as relevant here, appraise new cyber technology vendors.

62. NCR operates a secure, closed system that allows it to accurately test, as relevant here, cybersecurity software against simulations of real-world threats in order to provide vendors with important insight into a product's capabilities and market-readiness.

63. Vendors whose products are tested by NCR receive the test results, and an analysis of the test event is provided to the U.S. Army Combat Capabilities Development Command – Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance.

64. However, in the absence of disclosure by a vendor, customers across the wider federal government have no way of knowing that NCR conducted a test, let alone the results of a such a test.

65. As such, it is incumbent upon the vendor to maintain transparency by alerting government customers to NCR evaluations and the subsequent results.

66. NCR tested the Vectra Platform in late January and early February 2022.

67. NCR evaluators conducted a series of simulated attacks on a computer network protected by the Vectra Platform to test its ability to detect various adversarial actions, including network, scanning, exploit, and implant type attacks.

68. The results of the tests were awful: the Vectra Platform failed to detect many of the attacks and adversarial actions deployed by the NCR evaluators, including some threats that should have been detected by even the most basic threat-detection software.

69. Several notable detection failures involved persistent Command and Control connections, Lateral Movement, Beaconing, and Network Scans, all of which are among the types of threat activity that Vectra markets its product as being able to detect.

70. Specifically, Command and Control is a type of malicious computer networking activity involving connection between a remote Command and Control server operated by a threat actor and malware on an infected computer system or server. The distributed malware regularly attempts to check in with the C&C server to ensure continued unauthorized access, often over common ports and protocols which, while harder to detect, are behaviorally identified by several leading Endpoint Detection and Response and Network Detection and Response monitoring tools. If unnoticed, C&C beaconing can enable malicious activity including, but not limited to, privilege escalation, data exfiltration, and ransomware deployment.

71. Specifically, Lateral Movement is commonly achieved through abuse of Server Message Block (SMB) shared drives. SMB, a communication protocol for sharing access to files, printers, and other networked devices, is often used by administrators to conduct legitimate activities, such as deployment of tooling and file modification. SMB activity is often clearly visible in Windows Event Logs, and, if not detected by a monitoring solution, can lead to large volumes of data exfiltration, widespread endpoint compromise, and malware deployment. After obtaining unauthorized access and administrative permissions, adversaries can map SMB enabled folders to their own remote systems, supporting the propagation of malware.

72. NCR evaluators were called upon by the company to highlight the Vectra Platform's deficiencies in a post-test debriefing. During this post-test debrief, an NCR evaluator commented that he was surprised that the Vectra Platform had failed to detect some of the basic attacks.

73. Following this debrief, Stern consulted with one of Vectra's sales engineers to further discuss the results of the NCR test. According to the engineer, on a scale of one to ten, the flaws exposed by the NCR test were an "8+" in terms of severity.

74. Stern realized the gravity of the situation, given that the Vectra Platform was already deployed by defense and intelligence community customers and that

Vectra was part of then on-going major solicitations. He therefore understood that Vectra had a moral, ethical, and legal obligation to act to troubleshoot the problems with the Vectra Platform and, in the meantime, alert its current and prospective customers to them, especially those in the defense and intelligence spheres.

75. In early March 2022, Stern first aired his concerns with Sanders, his direct supervisor.

76. Stern requested that Vectra quickly identify the root cause(s) of the problems identified by the NCR testing and notify its current and potential federal government customers of the problems identified by NCR along with a plan of action and milestones ("POAM").

77. Sanders assured Stern that Vectra would work to solve the issues identified by the NCR testing but was reluctant to disclose the test results to existing customers and potential customers with whom Vectra was then in the process of negotiating contracts out of concern for the disruption to Vectra's business quarterly/annual sales commitments might cause.

78. Not willing to stand idly by, beginning in March 2022, Stern initiated a number of meetings and calls with Vectra's product development team in attempt to understand the root causes of the Vectra Platform's poor performance in the NCR test.

79. Stern initially consulted with Brad Woodberg, Vectra's Director of Product Development, in the second half of March 2022. He also later participated in several follow-on calls with members of Vectra's product development team.

80. Stern's concerns only intensified as a result of these communications, as Vectra's product development team was unable to adequately explain how or why the Vectra Platform performed so poorly in its NCR testing.

81. With no viable solution to the demonstrated weaknesses in the Vectra Platform on the horizon, Stern took the step of reporting the NCR test results and his concerns directly to Vectra's CEO, Hitesh Sheth, in a March 2022 e-mail. In the e-mail, Stern expressed that he had some serious concerns about the findings.

82. Sheth never responded to Stern's e-mail.

83. After Stern reported the NCR test results to CEO Sheth, Sanders forcefully instructed Stern that, going forward, he was not to discuss the matter with anyone and was not to put anything about it in writing.

84. Stern nevertheless continued to lobby Sanders to take corrective action, but Sanders continued to demur.

85. Stern also became aware around this time that Michael Wilson, Stern's counterpart at Vectra for sales to intelligence community customers, was in the process of negotiating a large-scale deal with General Dynamics Information

Technologies ("GDIT")—the prime system integrator for many intelligence agency programs—on behalf of a federal customer within the intelligence community.

86. Upon information and belief, Wilson was set to earn substantial commissions—as much as $500,000—if that deal closed.

87. Wilson was aware of the NCR test results and, when he and Stern discussed the poor performance of the Vectra Platform, he opaquely responded that "[w]ell, it could have been for a lot of reasons," and neglected to address Stern's stated concerns.

88. Like Sanders, Wilson seemed more worried about the potential loss of sales to Vectra—and his own loss of income from sales commissions—than he did about the potentially grave security risks posed by allowing the Vectra Platform to be deployed on networks vital to national security.

D. Vectra precipitously terminates Stern.

89. On June 3, 2022—the same day that Stern was set to notify Sanders that he had secured a sponsor agency to support Vectra for FedRAMP certification—Sanders called Stern to inform him that he was being fired.

90. Surprised by this abrupt and unexpected turn of events, Stern asked Sanders why he was being fired. Sanders told Stern he was being let go for "HR-related issues" and, when pressed by Stern to explain, said "maybe someday I'll tell you."

91. After this comment, Sanders dropped off the call and a Vectra HR representative concluded Stern's termination in a peremptory fashion.

92. Immediately afterwards, Stern called Aaron Bean, Vectra's Vice President of Human Resources, to seek an explanation for why he was being terminated, especially because Stern had received no warnings or admonitions of any kind from HR about any issues.

93. Indeed, to that point in his more than two-decade long career, Stern had never been formally reprimanded by an employer, let alone fired for "HR-related issues."

94. Bean admitted to Stern that he was unaware of any HR issues. Instead, Bean stated that, according to Sanders, Stern "wasn't a good cultural fit" and that Sanders wanted to "clear the decks" before the end of the federal fiscal year for a new Federal Sales Director.

95. Vectra cut off Stern's access to his company e-mail within minutes of his termination.

E. Vectra interferes with Stern's subsequent efforts to obtain employment.

96. By August of 2022, Stern had interviewed with one of Vectra's competitors, DarkTrace Holdings Ltd., for a position as their Sales Director for the Department of Defense and Intelligence Community.

97. Like Vectra, DarkTrace develops and markets cybersecurity detection software.

98. Stern was fully qualified for the job, given his many years of successful work selling software and other IT products and services to customers within the federal government, especially the Department of Defense.

99. Discussions between Stern and DarkTrace progressed to the point of negotiating compensation and determining a start date.

100. Although never reduced to writing, DarkTrace and Stern discussed Stern receiving a salary of approximately $350,000, exclusive of commissions and other benefits.

101. Suddenly and without warning, however, DarkTrace communicated to Stern that it was no longer interested in moving forward with hiring him.

102. When Stern asked Sally Grant—DarkTrace's Vice President – Federal and the individual at DarkTrace responsible for recruiting Stern—the reason for the sudden change, she commented that Stern was too "radioactive," that she had spoken with people from Vectra, and that she had concerns. When Stern pressed her to disclose the individuals she had spoken to, Grant asked Stern if he knew of a "Michael Wilson."

103. Grant further reiterated that Stern was "radioactive," "too hot with Vectra," and that she "didn't want any part of it."

First Cause of Action

[Violation of 31 U.S.C. 3730(h)]

104. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

105. Under 31 U.S.C. § 3730(h), an employer may not discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment because of lawful acts done by the employee, contractor, agent or associated others in furtherance of efforts to stop one or more violations of the False Claims Act.

106. Stern reported the serious deficiencies exhibited by the Vectra Platform during the NCR testing to his superiors at Vectra, in particular Sanders and Sheth.

107. In expressing his concerns to Sanders, Stern demanded that Vectra take corrective action, including remedying the deficiencies in the Vectra Platform and, until the problems with the Vectra Platform were corrected, notifying Vectra's current and potential customers within the federal government of the NCR test results.

108. Stern believed that the NCR test results—which demonstrated substantial weaknesses in the Vectra Platform—showed that deploying the Vectra Platform on computer networks within the defense and intelligence spheres posed a significant threat to national security, especially given recent, high-profile attacks on federal government systems, such as the 2020 "SolarWinds" data breach.

109. Stern reasonably believed that knowledge of the NCR test results, which demonstrated that the Vectra Platform might fail to alert users to significant cybersecurity threats, would be of great concern to Vectra's customers within the federal government, and that Vectra had a duty to inform those customers, who are charged with protecting national security and vital national cyber infrastructure, that the representations about the capabilities of the Vectra Platform on which they relied when contracting with Vectra were not accurate.

110. Furthermore, Stern reasonably believed that continuing to market the Vectra Platform to customers within the federal government, without disclosing the results of the NCR testing, would result in one or more violations of the False Claims Act because the significant weaknesses uncovered by the NCR testing would constitute material information to customers within the federal government, particularly the Department of Defense and the Intelligence Community.

111. Instead of taking corrective action, however, Vectra ignored and rebuffed Stern, with its senior management demonstrating greater concern for the short-term success of the business than for the risk of substantial danger to national security posed by deploying the Vectra Platform on defense and intelligence networks.

112. Ultimately, Vectra retaliated against Stern for his efforts by suddenly terminating his employment.

113. As a result of Vectra's actions, Stern has suffered, and continues to suffer, damages in an amount according to proof.

Second Cause of Action

[Violation of Cal. Labor Code § 1102.5]

114. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

115. California Labor Code § 1102.5(a) prohibits employers from discharging, retaliating, or in any manner discriminating against an employee for disclosing information to a person with authority over the employee, or to another employee who has authority to investigate, discover, or correct the violation or noncompliance, if the employee has reasonable cause to believe that the information discloses a violation of state or federal law, or a violation or noncompliance with a state or federal rule or regulation.

116. Labor Code § 1102.5(c) prohibits employers from retaliating against an employee for refusing to participate in an activity that would result in a violation of state or federal statute, or a violation or noncompliance with a state or federal rule or regulation.

117. Under the False Claims Act, 31 U.S.C. § 3729(a)(1)(B)-(C), it is unlawful to knowingly make, use, or cause to be made or used, a false record or statement material to a false or fraudulent claim, or to conspire to do so.

118. Separately, the federal acquisition regulations, specifically 48 CFR 52.203-13(b)(3), require federal contractors to make timely disclosure to the relevant agency's Office of the Inspector General whenever the contractor has credible evidence that one of its principals, employees, agents, or subcontractors has committed a violation of the False Claims Act.

119. Finally, federal defense acquisition regulations, specifically 48 CFR 252.204-7012, require contractors to report "cyber incidents," defined as "actions taken through the use of computer networks that result in a compromise or an actual *or potentially adverse effect on an information system and/or the information residing therein*." (Emphasis added).

120. Stern had reasonable cause to believe that Vectra's non-disclosure of the NCR test results to current and prospective federal government customers was a violation of Vectra's duty under the False Claims Act to not make materially false representations or omissions in connection with obtaining contracts with the federal government, and, furthermore, violated Vectra's obligations under federal acquisition regulations to disclose both cyber incidents and credible evidence of False Claims Act violations.

121. However, rather than take corrective action in response to Stern's reporting by disclosing the results of the NCR tests to its customers in the federal government, Vectra instead retaliated against Stern by firing him.

122. Upon information and belief, Sanders' decision to terminate Stern was ratified at the highest levels of Vectra's management at its headquarters in San Jose, California.

123. As a result of Vectra's actions, Stern has suffered, and continues to suffer, damages in an amount according to proof, but, in any event, in excess of $75,000.

Third Cause of Action

[Wrongful Termination in Violation of Public Policy]

124. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

125. Under California law, no employee, whether an at-will employee, or employee under a written or other employment contract, can be terminated for a reason that is in violation of a fundamental public policy. California courts have interpreted a fundamental public policy to be any articulable constitutional, statutory, or regulatory provision that is concerned with a matter affecting society at large rather than a purely personal or proprietary interest of the employee or employer. The public policy must be fundamental, substantial, and well established at the time of Plaintiff's discharge.

126. It was and is the public policy of the State of California, as set forth in California Labor Code § 1102.5, that an employer may not retaliate or in any manner

discriminate against an employee for making an oral or written complaint regarding illegal activity to a governmental agency or their employer.

127. Here, Vectra retaliated against Stern because he raised the alarm internally at Vectra about the significant weaknesses in the Vectra Platform exposed by the NCR testing and because of his efforts to encourage Vectra to comply with its obligation to disclose those weaknesses to its existing and potential customers within the federal government.

128. Upon information and belief, Sanders' decision to terminate Stern was ratified at the highest levels of Vectra's management at its headquarters in San Jose, California.

129. As a result of Vectra's retaliatory action, Stern has suffered, and continues to suffer, damages in an amount according to proof, but, in any event, in excess of $75,000.

Fourth Cause of Action

[Tortious Interference with Prospective Economic Advantage]

130. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

131. Stern had an economic relationship with DarkTrace in the form of a tentative employment opportunity which, if consummated, would have resulted in a substantial economic benefit to Stern.

132. Wilson, Vectra's Federal Advanced Programs Group Manager, knew about the relationship between Stern and DarkTrace by virtue of his conversation with Grant.

133. Wilson intentionally acted to disrupt the relationship between Stern and DarkTrace by making comments to Grant that led Grant to believe Stern was "radioactive."

134. As a direct consequence of Wilson's comments, DarkTrace inexplicably declined to move forward with hiring Stern.

135. As a consequence of the disruption of the relationship between Stern and DarkTrace, Stern has suffered, and continues to suffer, damages in an amount according to proof, but, in any event, in excess of $75,000.

Fifth Cause of Action

[Fraudulent Inducement to Contract]

136. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

137. Vectra, through Sanders and Davis, made material representations to Stern concerning the viability of the deals Stern would inherit upon joining Vectra and the status of Vectra's pursuit of FedRAMP certification.

138. Sanders and Davis knew these representations were false at the time they made them.

139. These representations were made intending that Stern would rely on them in deciding whether to accept Vectra's offer of employment.

140. Stern ultimately did rely on Sanders' and Davis' representations in deciding to accept Vectra's offer of employment.

141. As a result of Vectra's actions, Stern has suffered, and continues to suffer, damages in an amount according to proof, but, in any event, in excess of $75,000.

Sixth Cause of Action

[Negligent Misrepresentation – *In the Alternative*]

142. Stern re-alleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

143. Even if Sanders and/or Davis did not know their representations concerning Vectra's sales pipeline and FedRAMP certification were false, they nevertheless made those representations without any reasonable ground to believe that they were true.

144. These representations were made intending that Stern would rely on them.

145. Stern ultimately did rely on these representations when he accepted Vectra's employment offer.

146. As a result of Vectra's actions, Stern has suffered, and continues to suffer, damages in an amount according to proof, but, in any event, in excess of $75,000.

Dated: March 30, 2023

Respectfully submitted,

/s/ Bruce C. Fox

Bruce C. Fox (*pro hac vice forthcoming*)
bruce.fox@obermayer.com
Hugh T. McKeegan (*pro hac vice forthcoming*)
hugh.mckeegan@obermayer.com
OBERMAYER REBMANN MAXWELL & HIPPEL LLP
525 William Penn Place, Suite 1710
Pittsburgh, PA 15219
Tel: (412) 566-1500
Fax: (412) 281-1530

Chaka Okadigbo (CA State Bar No. 224547)
cokadigbo@hkm.com
HKM EMPLOYMENT ATTORNEYS LLP
700 S. Flower Street, 10th Floor
Los Angeles, CA 90017
Telephone/Facsimile: (213) 431-6209

Attorneys for Plaintiff Michael Stern